WEBSITE SECURITY POLICY

1 Policy Statement

To meet the enterprise's business objectives and ensure the continuity of its operations, _____ shall adopt and follow well-defined and time-tested plans and procedures, to ensure the integrity, availability, and authenticity of its website and all information contained within. An organization’s website is its interface with the external world. Information contained within the website is deemed as authentic statements from the management of the organization. It is imperative to publish only authenticated content on the website and maintain its integrity and availability.

2 Purpose

The purpose of the Security Policy is to establish rules for preserving the integrity, availability, and authenticity of _____ Website/App.

3 Scope

3. 1 Employee

This applies to all permanent employees, contractual employees, trainees, privileged customers, and all other visitors.

3.2 Documentation

The Security Policy documentation shall consist of the Security Policy and related procedures & guidelines.

3.3 Document Control

The Security Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.

3.4 Records

Records being generated as part of the Security Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

3.5 Distribution and Maintenance

The Security Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the Security Policy document shall be with the CISO and website administrator.

4. Privacy

The Security Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.

5 Responsibility

The CISO / designated personnel and website administrator are responsible for the proper implementation of the Security Policy.

6 Policy

Following are the policies defined for maintaining the Security of the website:

- The website shall be developed and maintained as per relevant guidelines of Govt. of_____
- User registration for secured access to the website shall be required when i) a web application or internal link requires user identification before processing, or ii) accessed data has been classified as “sensitive” and requires further authorization.
- To facilitate site management, the information shall be collected for statistical purposes. _____ shall employ software programs to compile summary usage statistics, which may be used for assessing what information is relevant to users. The data so accumulated may be used to help determine technical design specifications, identify system performance, or pinpoint problem areas.
- Except for authorized security investigations and data collection, no attempts shall be made to identify individual users or their usage habits. Accumulated data logs will be scheduled for regular deletion in accordance with schedules set by the web administrators.
- Unauthorized attempts to upload information or change website information are strictly prohibited and may be punishable under relevant cyber laws.
- Access to sensitive or proprietary business information on the websites shall be limited to employees, customers, clients, and vendors who have been determined to have an appropriate business reason for having access to such data. All registered website users, who are granted security access, will be identified by a user name (referred to as the User ID). All actions performed with a User ID will be the responsibility of the ID’s registered owner.
- Individuals who are granted password access to restricted information on the website are prohibited from sharing those passwords with or divulging those passwords to, any third parties. User will notify _____ immediately in the event a User ID or password is lost or stolen or if the user believes that a non-authorized individual has discovered the User ID or password.
- _____ records shall be final and conclusive in all questions concerning whether or not a specific User ID or password was used in connection with a particular action.
- Any data or document upload to social networking sites shall be duly authorized by the competent authority and shall be done by designated persons authorized to do so.

7 Enforcement

Any employee found to have violated this policy may be subjected to disciplinary action in line with the HR Policy.

Contact Us

If you have any questions about our Returns and Refunds Policy, please contact us:

- By visiting this page on our website: [WEBSITE_CONTACT_PAGE_URL]
- By sending us an email: [WEBSITE_CONTACT_EMAIL]